1-1-2010

The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market

Andy Jones
Security Research Centre, BTLondon, UK

Craig Valli
Edith Cowan University

Glenn S. Dardick
Edith Cowan University

Iain Sutherland
Edith Cowan University

G. Dabibi
Security Research Centre, BTLondon, UK

See next page for additional authors

DOI: 10.4225/75/57b2968040cdd
8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market

Andy Jones[1,2,3], Craig Valli[2], Glenn S. Dardick[2,4], Iain Sutherland[2,5], G Dabibi[1], Gareth Davies[5]

[1]Security Research Centre, BT
London, UK
[2] secau - Security Research Centre
Edith Cowan University
Perth, Western Australia
[3] Khalifa University of Science, Technology and Research,
Sharjah, United Arab Emirates
[4]Longwood University
Virginia, USA
[5] University of Glamorgan
UK
andrew.jones@kustar.ac.ae

Abstract

The ever increasing use and reliance upon computers in both the public and private sector has led to enormous numbers of computers being disposed of at the end of their useful life within an organisation. As the cost of computers has dropped, their use in the home has also continued to increase. In most organisations, computers have a relatively short life and are replaced on a regular basis with the result that, if not properly cleansed of data, they are released into the public domain containing data that can be relatively up to date. This problem is exacerbated by the increasing popularity and use of smart phones, which also contain significant storage capacity. From the results of the research it remains clear that the majority of organisations and private individuals that are using these computers still remain ignorant or misinformed of the potential volume and type of information that is stored on the hard disks contained within these systems. The evidence of the research is that neither organisations nor individuals have considered, or are aware of, the potential impact of the information that is contained in the disks from these systems becoming available to an unintended third party.

This is the fifth study in an ongoing research programme being conducted into the levels and types of information that remain on computer hard disks that have been offered for sale on the second hand market. This ongoing research series has been undertaken to gain an understanding of the level and types of information that remains on these disks, to determine the damage that could potentially be caused if the information was misused, and to determine whether there are any developing trends. The disks used have been purchased in a number of countries. The rationale for this was to determine whether there are any national or regional differences in the way that computer disks are disposed of and to compare the results for any regional or temporal trends. The disks were obtained from a wide range of sources in each of the regions in order to minimise the effect of any action by an individual source.

The first study was carried out in 2005 and since then has been repeated annually with the scope being incrementally extended to include additional research partners and countries. The study in 2009 was carried out by British Telecommunications (BT) and the University of Glamorgan in the UK, Edith Cowan University in Australia, Khalifa University in the United Arab Emirates and Longwood University in the USA.

The core methodology of the research has remained unaltered throughout the duration of the study. The methodology has included the acquisition of a number of second hand computer disks from a range of sources and determining whether the data contained on the disks has been effectively erased or if they still contain information relating to previous owners. If information was found on the disks from which the previous user or owner could be identified, the research examined whether it was of a sensitive nature or in a sufficient volume to represent a risk. One of the consistent results of the research through the entire period has been that, for a significant proportion of the disks that have been examined, there was sufficient information present to pose a risk of a compromise of sensitive information to either the organisation or the individual that had previously used the disks. The potential impacts of the exposure of this information could include embarrassment to individuals and organisations, fraud, blackmail and identity theft. In every year since the study started, criminal activity has also been exposed. As has been stated in the previous reports, where the disks had originated from organisations, they had, in many cases, failed to meet their statutory, regulatory and legal obligations.

In the 2009 study, the fifth in the series, the research methodology that had been followed in the previous studies was repeated, but in addition Khalifa University of Science Technology and research contributed to the analysis of the disks.

Keywords
Computer forensics, disk analysis, data recovery, data disposal, data destruction, data leakage, privacy.

INTRODUCTION

This research series was initiated in January 2005 (Jones et al, 2005). The results of the first study revealed that a significant proportion of the disks that were examined still contained large amounts of information, in many cases sensitive, from which the previous owner or user could be identified. Prior to the publication of this first study report there had been limited research into this subject, with the most significant findings being reported by (Garfinkel and Shelat, 2003). There had been a small number of limited surveys conducted or sponsored by vendors and a number of newspaper reports on the discovery of personal data found on disks that had not been correctly disposed of. This first study report showed that the majority of the disks that were obtained still contained significant quantities of sensitive information that the researchers considered had the potential to cause embarrassment or financial harm to either the organisation or the individual.

As in the previous years, all of the research has been conducted under the same conditions (using commonly and easily available tools that have similar capabilities) and the results then compared. The recommendations that have been made as a result of the research are on ways in which the destruction or erasure of data from disks that were being disposed of could be improved.

This paper, the report on the fifth and latest survey, contains the results of the 2009 research which has had the same objectives as the research in the previous years. The research was again sponsored by British Telecommunications (BT) and Sims Lifecycle Services.

THE RESEARCH

Throughout the duration of the research, in order to maintain consistency, the same objectives, processes and procedures that were used in the original study have been followed. Other studies have been spawned by the research, including a “dead disk” study that is currently ongoing at the University of Glamorgan, where disks that were not working when originally tested have had further extensive testing and investigation to determine the causes of the failures and the level of difficulty that recovery of the data contained would entail. Throughout the entire period, all of the disks used in the research were purchased at computer auctions, computer fairs or through eBay in the respective regions. The disks were acquired discretely and in small batches by a number of purchasers so that the sellers would not have any indication of the reason for purchases. A second reason for purchasing the disks either singly or in small batches was to minimise any influence that the practices of one seller might have had on the overall results.

In 2009, consistent with the research in each of the previous years, the disks were supplied “blind” to the researchers so that they had no external visual indicators of the potential source of the disks. The only markings on the disks that the researchers were provided with were sequential serial numbers so that each disk could be uniquely identified throughout the process. By supplying them in this way, any information that is recovered by the researchers could be clearly identified as having been the result of the data that was available on the disk.

The research methodology remained unchanged from earlier research (Jones 2005, 2006, 2008) with each disk being forensically imaged using verified software and then placed in a secure storage container. All subsequent analysis was undertaken on the forensic images. The rationale for this time consuming step remained unchanged from previous years and was to meet two requirements. The first was the need to preserve the original media in an unaltered state and store it in a secure area in case reportable criminal activity was detected and there was a requirement to pass the disks on to the police. The second reason was to allow the research to be carried out in a non-intrusive manner that did not affect or change the original data in case any anomalies were detected with the image and it was necessary to validate the data against a second image created from the original. As in previous years, this proved to be a sensible precaution, as two of the disks were found to contain material that necessitated them being handed over to law enforcement for further investigation.

The tools used in the 2009 study were fundamentally the same as those used in the previous years (although the versions of the tools may have changed). The tools performed similar functions to the Windows Unformat and

Undelete commands and that of a hex editor (which was used to view any information that exists in the unallocated portions of the disk). All of the tools that perform this type of functionality are freely available: examples include the Linux based Autopsy (Version 2.24) and The Sleuth Kit (version 3.1.3)[29] software. These types of tools do not require significant levels of skill or knowledge to effect the recovery of remnant data from storage media and there are now numerous online tutorials for operation of these tools for the purposes of data recovery. The objectives have remained the same as in previous years: firstly to determine if the disks had been effectively cleansed of data, secondly, if they still contained information, whether it was either visible or easily recoverable with the tools identified above. The third objective of the research was to determine whether the information present on the disk would allow for the identification of the organisation or individual(s) that had used the disk's host computer. The results of the 2009 survey indicate that, over the last five years, there has been small but consistent improvement in the proportion of the disks that contain sensitive organisational or personal information that are made available in the second-hand market. Before detailing the results of the 2009 survey, the results of the studies in the preceding years are briefly described below.

SUMMARY OF THE PREVIOUS RESEARCH RESULTS

Over the whole of the period of the series of studies, one of the issues that has been highlighted is the fact that, to date, nearly half of the second hand disks that were obtained and could be accessed, have had some attempt made to remove the data. In the majority of these cases, the attempts were unsuccessful. The majority of those disks contained data that could easily be recovered by either connecting the disk to another computer or through the use of the basic tools that are described elsewhere in this paper. In the majority of cases, these disks contained sufficient data to allow the previous owner, whether an organisation or an individual, to be identified. Around twenty percent of the disks contained financial information relating to organisations, including staff salary details, sales receipts and profit and loss reports. A number of the disks could be identified as having been used in the organisations that were part of the critical infrastructure such as power generation, water and telecommunications utilities. Throughout the period of these studies, there has been an increasing awareness of the impacts of data breaches, data losses and identity theft that has come about as a result of regular publicity of incidents together with the publication of the results of a number of surveys and reports (Price Waterhouse Cooper, 2006, 2008; Johannes, 2006; Verizon, 2008, 2009, 2010; ITRC, 2008, 2009, 2010).

THE 2009 RESEARCH RESULTS

This section details the results for the research carried out during 2009, from the disks that were obtained in the UK, the USA, Germany, France and Australia. As in previous years, the results of the study are broken down into the individual countries to enable comparison.

For the 174 disks obtained in the UK:

- 60 (34% of the disks) were physically damaged and could not be accessed.
- 32 (18% of the readable disks) had been wiped and contained no data.
- Of the remaining 82 (47 % of the readable disks)[30],
  - 28 (34%) contained sufficient information for the organisation that they had come from to be identified.
  - 36 (45%) contained sufficient information for individuals to be identified.
  - 18 (22%) indicated that attempts had been made to remove data from the disks by deletion, formatting or reinstallation of an operating system.
- 2 (2% of the readable disks) contained information that was considered to be illicit.

For the 74 disks that were obtained from North America:

- 13 (18% of the disks) could not be accessed
- 23 (38% of the readable disks) had been wiped and contained no data.
- Of the remaining 38 (62% of the readable disks),

1 The Sleuth Kit, http://www.sleuthkit.org/index.php

30 The three categories in this section are independent of each other. A disk may contain information on just an individual or an organisation or both and any of them may also have had attempts made to remove the data.

  - 14 (37%) contained sufficient information for the organisation that they had come from to be identified.
  - 18 (47%) contained sufficient information for individuals to be identified.
  - 10 (26%) indicated that attempts had been made to remove data from the disks by deletion, formatting or reinstallation of an operating system.
- 6 (10% of the readable disks) contained information that was considered to be illicit.

For the 39 disks that were obtained from Germany:

- 8 (21% of the disks) were not in working order and could not be accessed.
- 16 (41% of the readable disks) had been wiped and contained no data.
- Of the remaining 15 (38% of the readable disks),
  - 4 (26%) contained sufficient information for the organisation that they had come from to be identified.
  - 3 (20%) appeared to be from individuals.
  - 3 (20%) indicated that attempts had been made to remove data from the disks by deletion, formatting or reinstallation of an operating system.

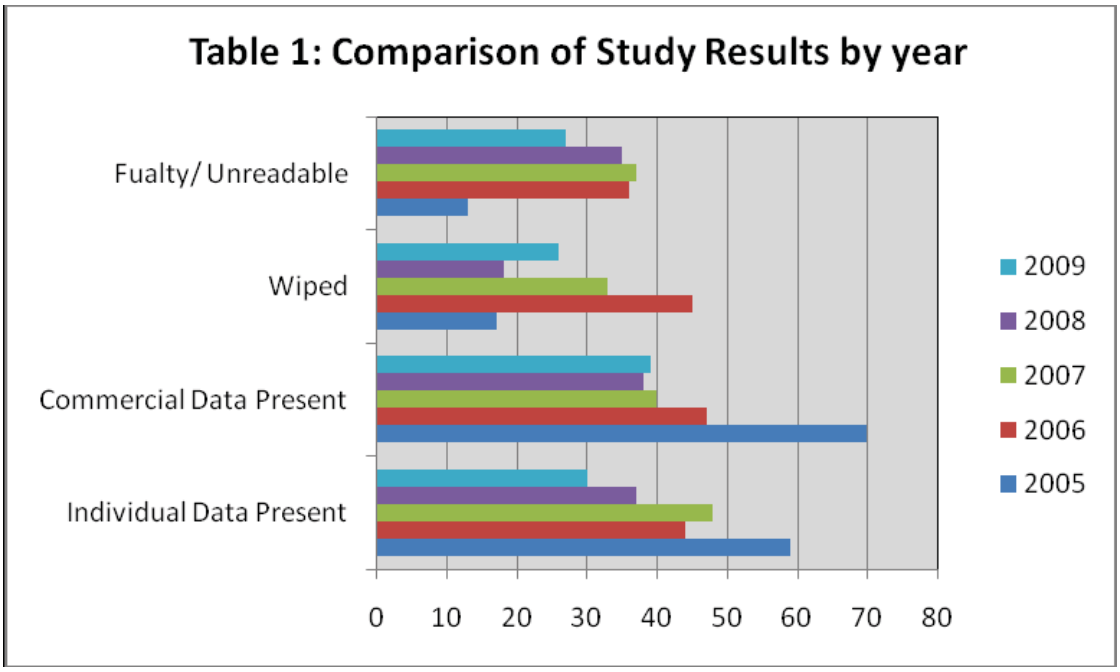
For the 17 disks that were obtained from France:

- 8 (47%) of the disks were physically damaged and could not be accessed
- 4 (24% of the readable disks) had been wiped and contained no data.
- Of the remaining 5 (29%),
  - 1 (20%) contained sufficient information for the organisation that they had come from to be identified.
  - 1 (20%) contained sufficient information for individuals to be identified.
  - 3 (60%) indicated that attempts had been made to remove data from the disks by deletion, formatting or reinstallation of an operating system.

For the 42 disks that were obtained from Australia:

- 5 (12%) of the disks were physically damaged and could not be accessed
- 14 (33% of the readable disks) had been wiped and contained no data.
- Of the remaining 23 (55%),
  - 18 (78%) contained sufficient information for the organisation that they had come from to be identified.
  - 6 (26%) contained sufficient information for individuals to be identified.

Table 1 shows a comparison of the results for each of the annual disk surveys.



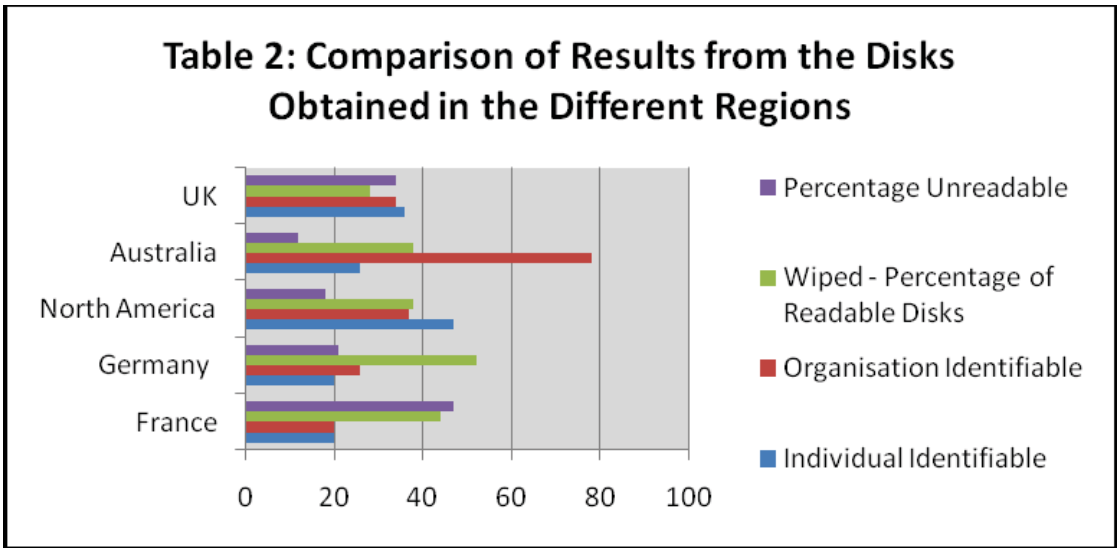
Note: The results for the wiped disks are given as a percentage of the disks that were readable.
Note: The results for data present are given as a percentage of readable disks that had not been wiped.

The results of the 2009 survey appear to indicate that there is a consistent improvement in the results in the majority of the areas measured over the period. There has been consistent improvement in the reduction of both commercial and personal data found over the whole period. It is interesting and a matter of concern to note that, while there has not been consistency, the general proportion of disks that have been wiped of all data has also reduced over the period.

Comment: The disks that are obtained for the study are selected from the widest possible range of sources. It was noted by the people responsible for the procurement of disks in the USA that there had been a noticeable increase in the number of disks offered for sale in the USA that were advertised as having been wiped. Because these were specifically advertised as having been wiped, such disks were not procured for the study as they were no longer considered to be part of the generic „random" group of disks that were available. In the future, such disks will be included in order to ensure that the overall study results are not distorted and also to give a view on the effectiveness of the methods used to wipe the disks.

The trend that had been previously noted, with the exception of the 2005 results, in the proportion of the disks that were faulty/unreadable has continued and, the level has now declined over the period from 2006 to 2009 from 36% to 27%.

Table 2 below shows a comparison of the results obtained during the 2009 study from the disks acquired in the different regions.



Note: The results for the wiped disks are given as a percentage of the disks that were readable.
Note: The results for data present are given as a percentage of readable disks that had not been wiped.

The results of the 2009 survey by individual regions have again revealed what appears to be a number of disparities between the regions. The number of disks that were obtained that were unreadable still varies considerably. The numbers this year ranged from 12 percent in the Australia to 47 percent in France.

The second disparity that was noted was that while the general trend in the level of data from which an organisation could be identified has consistently reduced over the period, there was a noticeable increase in the proportion of disks from Australia that contained such information. The results from the study this year found that 61 percent of disks that were readable and had not been wiped contained sufficient information for the organisation that they had been used by to be identified. Last year the results for Australia were also high with 60 percent.

Over the period of the last five years there are clear indications that there are trends developing that the numbers of disk that contain information relating to organisations and individuals is reducing. Unfortunately, it has also been noted that because of the increasing volume of storage capacity of the disk, where such data is found, the quantity appears to be increasing.

An indication of the quantity and type of material that was recovered during the 2009 research includes disks that originated in local government, the healthcare sector, commercial and the media. Examples of the type of data recovered include:

One disk from the UK contained information from a local council. This included numerous documents that appear to have originated within the payroll department at the organisation. The documents include some of the following details, which were relevant up to 2008:

- Automatic credit recall letter to the Royal Bank of Scotland
- Account numbers and sort codes used by the various departments within the Council
- Names, addresses, payroll numbers, amounts paid and various other details relating to employees at the organisation
- Emails detailing specifics of the individual circumstances of employees, including sick-pay arrangements, queries regarding over and under-payments and finance requirements
- Details of queries made to the Royal Bank of Scotland regarding the organisation's accounts

Additionally, a number of encrypted Microsoft Access databases were recovered and decrypted by the analysts involved in this study. They each used the same weak password for decryption, and while they were apparently empty, the names of individual tables and fields within the databases suggest that they would have been used to store a wealth of valuable information. Their structure also suggests that they were intended to be used by more than one software applications.

A disk recovered in the UK was from a computer supply company. The information contained on the disk included details of contracts to supply computers to local councils in the UK. The details included full specifications for computing and networking equipment, as well as a complete network topology and full addressing details, as well as the usual order and shipping information.

A disk recovered in the UK had originated in a direct marketing company. The disk contained documents that gave details of the breakdowns of calls from the broadband users of a major Internet Service provider, complete with details regarding which departments within the service provider handled which calls, and the sales and conversation rates achieved by each. These were complemented by a large body of training material marked as being provided by a subsidiary of the service provider.

Another disk recovered in the UK from a media supply company contained a large number of documents revealing details of computer and software systems delivered to the company's customers. These details include computer specifications, details of the software systems in use on them, the layout and architecture of the databases used by the customers, and complete network topologies of the deployed systems. These were complemented by lists of IP address mappings, including mappings of domain names to public IP addresses, and public IP addresses to internal network topologies.

One disk was recovered that originated from a telecommunications company in the UK. Included in the material recovered were details of a merger with another communications carrier that had taken place in 2004 and a large number of documents that included:

- Itemised telephone bills
  - Names of account holders
  - Addresses of account holders
  - Account numbers of account holders
  - Invoice numbers
  - Telephone numbers held by account holders
  - Full call histories for each billing period

- Letters to customers
  - Names, addresses, phone numbers of account holders
  - Account termination details
  - Port Authorisation Codes (PAC) for transferring numbers

- Lists of customers
  - Names, phone numbers, addresses of account holders
  - Contract periods
  - PAC codes
  - Last four digits of credit card used to pay bills

- List of business accounts
  - Name of business holding account
  - Number of phone numbers held by each account

One disk recovered in the UK had originated from an International Design Consultancy. This disk contained a number of documents relating to specific jobs undertaken by the consultancy. The individual user of the disk could be identified from these, and full details of the prices charged for the jobs were included. Other documents recovered included some documents marked as "CONFIDENTIAL", numerous CVs, and spreadsheets detailing the use of expenses. Additionally, a global contact list was identified that appeared to hold the names, phone numbers, and email addresses of contacts within a large number of companies that the disk holder presumably worked with.

Another disk that was recovered in the UK from a specialist recruitment agency contained a large number of documents from the period 2003-2007. The details held in these documents are summarised below:

- A large number of CVs
- Database of employees – Names, addresses, contact information, etc.
- Databases of skill sets – Names, addresses

- List of addresses used for mailshots
- Details of bank charges incurred
- Cash-flow spreadsheets
- Commission calculations for employees
- Bank reconciliations
- Direct debits maintained by the organisation
- Invoice breakdowns
- Details of corporate credit card usage
- Details of petty cash usage
- Details of wages paid to employees

A disk that was recovered in Australia was from a major Australian television network and contained a number of confidential documents. The drive had been simply removed from an array and no effort had been made to remove the data. It disclosed the personal phone numbers of members of parliament, internal memos, story lines and a range of highly confidential material. These documents included a diary of staff member who felt they were being bullied in the work place, documents on staff performance, scheduling for shows and letters of invitation for various dignitaries and public figures. The files on the drive were as new as 2 months at time of purchase.

Another disk from Australia was from a major Australian accounting firm. It contained tax file numbers, customer data, letters of advice, letters of tax rulings, peoples personal income, personal asset base and company and business data. It contained the type of confidential data one would expect to find in a tax and accounting firm. The files found amount to a very serious breach of customer confidentiality. The drive again had been removed from an array with no attempt to cleanse the data.

Another set of disks from Australia was from a major Australian medical services company. The disks storage capacity was large (500GB) and contained a significant quantity of patient data including tests, test outcomes, letters of advice and of course extensive personal medical histories of ongoing patients. This data was extensive and highly confidential. In addition it contained business data relating to the practices it managed in a metropolitan area. This included doctors billing rates, profitability and other financial performance data relating to doctors performance. There were also various performance evaluations of these doctors. These disks had simply been formatted and no real attempt had been made to cleanse the data.

A disk recovered in Australia that had been formatted had evidence of home user activity (Gameboy ROMS and manuals), however it also appeared to have previously belong to a major chemicals company and had applications for approvals for pesticides and herbicides as well as internal memos, field trial data and information on upcoming products. Sales and marketing information was also present.

A disk recovered in Australia that had been formatted had belonged to a manager for a major IT Services company. Both corporate and personal financial documents were present. A number of Spreadsheets, some password protected were also found and were recoverable. The data in the spreadsheets referred to processing orders and instructions for batch processing for a financial institution.

In addition to the apparently corporate-owned disks summarised above, a number of disks that appear to have belonged to personal users were identified. The information recovered from these disks was somewhat similar in every case, and is summarised neatly by the following examples:

On one disk the documents recovered revealed the user"s name, occupation, the specific organisation and address at which they worked, as well as telephone numbers, email addresses, a complete employment history and details of their personal education. A large amount of personal email was also recovered.

Another disk contained the user's name, address and personal details were recovered from documents found on the disk, as well as a CV, a personal diary, and a significant amount of pornographic material. Additionally, web pages recovered from the disk reveal the last five digits of two credit card numbers, as well as their associated expiry dates and cardholder names.

On another disk, the user's name, address, employment details and complete CV were recovered from the disk. A large amount of corporate email from the user's workplace was identified, much of which included the contact details of individuals within the company. Additionally, several conversations with application programmers

were identified in which the details of software behaviour were described and in some cases the actual code was found to have been communicated via these email messages.

On another disk, the user's personal details were identified from documents recovered from the disk, as well as some details relating to individual jobs undertaken, online auctions won, and a significant amount of pornographic material. Additionally, a large body of personal email was identified, including some specific examples from online services that emailed the user's password to them in plaintext.

In addition to these examples, one personal disk was analysed that was found to contain pornographic images involving children. Upon identification of these images, analysis was suspended and the disk was immediately handed over to the police.

Data security breaches have continued with increasing regularity and are reported in the press on a very regular basis. The (ITRC, 2009) report indicates that the level of breaches reported has dropped from a peak of 656 reported breaches at the end of 2008 to 498 in 2009. Unfortunately, by October 2010, the same source reports that 580 breaches have already been recorded, which would indicate that the general trend in the number of breaches continues to increase.

In the previous reports, it was highlighted that the subject of the disposal of disks on which the data has not been effectively destroyed first made the news in the Canadian Globe and Mail (Canadian Globe and Mail, 1993) and that the subject has been reported with increasing frequency in the intervening years to date. The reports that appear in the press normally relate to high profile data losses. Within the last year, reports have included:

From the UK:

A (BBC News, 2010) report on a fine imposed on Zurich Insurance of £2.3m over the loss of customers' data. The UK operation of Zurich Insurance was fined by the Financial Services Authority (FSA) for losing the personal details of 46,000 of its customers. The information that was lost during a routine transfer to a data storage centre in South Africa included, in some cases, bank account and credit card information. The information went missing in August 2008, but Zurich did not become aware of the loss until a year later, when it then began notifying customers.

An (ICO, 2010) report from the UK Information Commissioner's office that there had been 464 security breaches reported to them during the year 2009-10. This compared to 434 in the previous year and 277 in the year before that.

A (BBC News, 2009) report that three of the HSBC firms have been fined in excess of £3m by the Financial Services Authority (FSA) for failing to adequately protect customers' confidential details from being lost or stolen after it was reported that information had been lost in the post on two separate occasions. The FSA cited concerns that it had found that "large amounts" of unencrypted customer details had been sent via post or courier to third parties. The FSA also stated that confidential information about customers was also found on open shelves or in unlocked cabinets. The failures were attributed to staff not having been given sufficient training on how to identify and manage risks such as identity theft.

A (Kouns, 2010) article on a report from the Ministry of Defence that it had had 1,705 data loss incidents had occurred during the period from 2005 to 2009.

An (Infosecurity, 2010) article that British firms had been warned over laptop data lethargy in a recently completed survey by Absolute Software. They survey reports that around two-thirds (65%) of IT managers have no idea where their organisation's mobile devices are, and that almost half of respondents are unable to manage PCs and Macs together.

From France:

According to the (Ponemon, 2009) report, the worst data breach in France last year cost an unidentified company 6.4 million Euros. The recently released report - French Cost of a Data Breach, revealed that each item of data lost in France cost an average of 89 euro.

From the USA:

A (Singel, 2009) report that an investigation was underway into the possible compromise of the records of 70 million veterans that put them at risk of identity theft. The issue related to a defective hard drive that the National Archives and Records Administration (NARA) had sent back to its vendor for repair and recycling without first destroying the data.

An Article from (AlertsecXpress,2010) reported that the parent company of American Airlines, AMR had suffered from one of the largest and possibly the most severe data breach incidents in this year when a computer disk was stolen from the Texas based corporate headquarters of AMR. The disk contained sensitive information on over 79,000 current, former and retired employees. The drive contained images of microfilm files, with names, addresses, dates of birth, Social Security numbers and a "limited amount" of bank account information and possibility also health insurance information.

An Article by (Westervelt, 2009) stated that Health Net Inc. had reported a healthcare data security breach that resulted in the loss of patient data, affecting 1.5 million customers. The managed healthcare provider stated that the lost portable external hard drive contained files, a mixture of medical data, Social Security numbers and other personally identifiable information on 446,000 Connecticut patients.

An Article by (Von Bergen, 2010) reported that a hard drive from a portable computer belonging to the Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan had been lost. The drive was believed to hold up to 280,000 names, address and health information of Medicaid members in Pennsylvania. The companies stated that the portable computer hard drive, which was used at community health fairs, was lost within the companies' corporate offices.

From Australia:

A report (Kouns, 2010a) on the exposure of user information by the Australian Broadcasting Corporation (ABC). The report stated that ABC had sent an email to players of its latest augmented reality (AR) game "Bluebird", saying that names, email addresses and passwords of 880 players of the game were available for download via an archive. The problem remained in place for almost a month.

A report by (Gedda, 2009), that many Australian government agencies did not have appropriate controls covering the use of portable storage devices (PSDs) for the handling of personal information. According to new research by the Office of the Privacy Commissioner, this personal information is being lost at an alarming rate. According to the report, more than 58% of agencies have experienced the loss or theft of an agency-issued PSD within the past 12 months.

As has been reported in earlier studies, before 2005 the subject of data losses was only reported in the mainline news once every two or three years. In the USA alone in 2009 there were 498 (ITRC, 2009) reports of data losses. One feature that is worth noting is that despite an apparent reduction in the total number of losses, the number of records disclosed has increased significantly. This is thought to be a result of the increasing storage volumes of the disks being disposed of.

The study this year has reinforced the findings of those in the preceding years, and while there is a trend of an improving situation with regard to the release of personal and corporate data there are still a significant number of disks found that contained sensitive information. The potential effect of the failure of organisations and individuals to properly remove or destroy sensitive information on disks that are disposed of is that this information is accessible to the purchasers of the disks and may cause embarrassment, potential financial losses and leave the original owner susceptible to blackmail or provide the opportunity for identity theft.

CONCLUSION

The improvements in the results that were noted over the last four years have largely been confirmed, with a small but steady reduction on the proportion of the disks that contain information from which an organisation or an individual can be identified. The number of disks that had been wiped has shown no consistent pattern over the period and it is difficult to draw any meaningful conclusion from the results other than that they are consistently lower than should be expected.

There is clearly an ongoing requirement for improvements in the education and awareness of staff within

organisations of the potential risks of data leaking into the public domain and of the actions that should be taken to ensure the safe removal or destruction of information stored on computer disks. It is also clear that at the individual, home user level, people still do not realise the risks that the disposal of computers and the disks that they contain pose and that many do not know how to securely dispose of the data.

It is increasingly difficult to believe, given the levels of publicity that the issue has received, that neither organisations nor individuals are aware of the potential problems that can occur when failing to take suitable measures for the destruction or removal of data. It is therefore likely that the results of the study are, at least in part, a result of;

a. The time it takes to organisations to develop, validate, implement and promulgate the new processes and procedures required to address the issues.
b. An ongoing lack of commitment or the structure to implement education and awareness campaigns at the levels that are required.
c. A failure to understand the problem at an organisational and governmental level and a failure to prioritise the issue.

RECOMMENDATIONS

Throughout the period that this research has been taking place, a number of recommendations have been made and reiterated regarding the measures that can be taken by both organisations and individuals to reduce the level of sensitive information that is released when disposing of computer devices and their hard disks. These are again detailed below, together with new recommendations:

- User Education - A public awareness campaign by Government, the media, commerce and/or academia. An example of this is the information provided by the disk manufacturer Seagate in their "Drive Disposal Best Practices[31] " documents or documents containing advice such as "How to Permanently Erase Data from a Hard Disk"[32]. Organisations such as the SANS Institute now provide courses such as the "Security 565 - Data Leakage Prevention"[33] course.

- Risk Assessments – Carry out risk assessments for the organisation to determine the level of sensitivity of the information that has been and is currently stored on disks.

- Best Practice - The introduction into organisations of procedures to ensure that computer systems and computer hard disks are disposed of in an appropriate manner. Examples of this include the Cornell University Best Practices for Media Destruction[34] and the Enterprise Strategy Group White paper on Information-Centric Security and Data Erasure[35].

- Data Erasure – The development of tools such as Blancco data erasure tool[36] or the Disk Doctors Data Sanitizer tool[37] and access to facilities to enable individuals to effectively remove the information from their computers.

- Physical Destruction - Where appropriate, the physical destruction of disks that have contained sensitive information using services such as the Ultratec Secure Data Erasure service[38] or that offered

[3] Seagate - Drive Disposal Best Practices, http://www.seagate.com/docs/pdf/whitepaper/Disposal_TP582-1-0710US.pdf (Accessed 24 Aug 2010)

[32] Sedory, DB (2008), How To Permanently Erase Data from a Hard Disk, http://mirror.href.com/thestarman/asm/mbr/WIPE.html (Accessed 15 Sept 2010)

[33] SANS Security 565 Course - Data Leakage Prevention, http://www.sans.org/security-training/data-leakage-prevention-in-depth-1372-mid (Accessed 15 Sept 2010)

[34] Cornell University Best Practices for Media Destruction, http://www.cit.cornell.edu/security/depth/practices/media_destruct.cfm (Accessed 20 Aug 2010

[35] Enterprise Strategy Group White paper on Information-Centric Security and Data Erasure, http://www.emc.com/collateral/analyst-reports/esg-wp-emc-security-jul-06.pdf (Accessed 15 Sept 2010)

[36] Blancco - http://www.blancco.com/en/ (Accessed 16 Sept 2010)

[37] Data Sanitizer - http://www.diskdoctors.net/data-sanitizer/software.html

[38] Ultratec Limited - http://www.ultratec.co.uk/services/dataerasure.asp (Accessed 15 Sept 2010)

by DataTerminators[39] or Blancco data destruction services[40].

- Encryption - The full or partial encryption of hard disks to ensure that information cannot be easily recovered. This can be achieved by using software such as TrueCrypt[41], PGP whole disk encryption[42] or the IdooSoft USB encryption tool[43] or hardware encryption devices such as the Secure Data Vault[44].

- Asset Tracking - Organisations may be able to more effectively secure their data if asset tracking was conducted at a storage device level. While this would involve the tagging of disks within the computers, it would allow for the individual items of storage media to be tracked. It is accepted that this would be a time consuming process but it would allow for the tracking of each item of storage media.

- Legal – Assign responsibility to those charged with managing the disposal of discarded or damaged hard disks. Disks found to be faulty should have the same disposal practices applied to them as disks removed from a working system. Develop processes for the return of disks still under warranty to the manufacturer.

ACKNOWLEDGEMENTS

In addition to the individuals named as authors for this paper, we would like to acknowledge the significant efforts of a number of people who assisted in the imaging and analysis of the large number of disks required for the research and the preparation of this report. The people involved were:

Andrew Woodward, Thomas Martin and Konstantinos Xynos.

REFERENCES

AlertsecXpress (2010), AMR Data Breach: 79000 Employees info at risk, 12 Jul 2010, http://blog.alertsec.com/2010/07/amr-data-breach-79000-employees-info-at-risk/ (Accessed 12 July 2010)

BBC News (2008), HSBC loses customers' data disc, http://news.bbc.co.uk/2/hi/7334249.stm (accessed 20 Oct 2010)

BBC News (2009), Previous cases of missing data, http://news.bbc.co.uk/2/hi/uk_news/7449927.stm, (accessed 20 Oct 2010)

BBC News (2010), Zurich Insurance fined £2.3m over customers' data loss, 24 Aug 2010, http://www.bbc.co.uk/news/business-11070217, (accessed 20 Oct 2010)

Canadian Globe and Mail (1993), Disk Slipped Into Wrong Hands, Canadian Globe and Mail, 2 Aug 1993. (Accessed 25 Feb 2009)

Garfinkel S.L, Shelat A, (2003), Remembrance of Data Passed: A Study of Disk Sanitization Practices. IEEE Security & Privacy, Vol. 1, No. 1, 2003.

Gedda, R., Govt agencies losing portable data: Privacy Commissioner, Techworld, 08 May 2009, http://www.techworld.com.au/article/302500/govt_agencies_losing_portable_data_privacy_commissioner, (Accessed 12 July 2010)

[39] DataTerminators - http://www.data-terminators.co.uk/ (Accessed 16 Sept 2010)

[40] Blancco Data destruction services - http://www.dataerasure.com/physical_destruction.htm (Accessed 15 Sept 2010)

[41] TrueCrypt - http://www.truecrypt.org/downloads.php (Accessed 16 Sept 2010)

[42] PGP Corporation, Whole disk encryption - http://www.pgp.com/products/wholediskencryption/index.html (Accessed 16 Sept 2010)

[43] IdooSoft USB Encryption tool - http://www.idooencryption.com/how-to-encrypt-usb.htm (Accessed 20 Sept 2010) 16 Secure Systems Secure Data Vault - http://www.securesystems.com.au/ (Accessed 20 Sept 2010)

[44] Secure Systems Secure Data Vault - http://www.securesystems.com.au/ (Accessed 20 Sept 2010)

Identity Theft Resource Centre (ITRC). (2008), Security Breaches 2008, http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, (Accessed 16 Sept 2010)

Identity Theft Resource Centre (ITRC). (2009) 2009 ITRC Breach Report, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202009.pdf (Accessed 16 Sept 2010)

Identity Theft Resource Centre (ITRC). (2010), 2010 ITRC Breach Report, http://www.idtheftcenter.org/ITRC%20Breach%20Report%202010.pdf (Accessed 16 Sept 2010)

Information Commissioner's Annual Report 2009/10, http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf, (accessed 24 Sept 2010)

InfoSecurity, British firms warned over laptop data lethargy, 12 October 2010, http://www.infosecurity-magazine.com/view/13141/british-firms-warned-over-laptop-data-lethargy/, (accessed 24 Sept 2010)

Johannes, R. (2006), The Demographics of Identity Fraud: Through education and vigilance, banks can prepare and protect those most vulnerable, Javelin Research, http://www.javelinstrategy.com/uploads/607.R_2006_IDF_Demographics.pdf, Aug 2006. (Accessed 04 Aug 2010)

Jones, A., Mee, V., Meyler, C., and Gooch, J,(2005), Analysis of Data Recovered From Computer Disks released for sale by organisations, Journal of Information Warfare, (2005) 4 (2), 45-53.

Jones, A., Valli, C., Sutherland, I., and Thomas, P,(2006), The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, Journal of Digital Forensics, Security and Law, (2006) 1 (3), 23-36.

Jones, A., Valli, C., Sutherland, I., and Dardick, G., (2008), The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, International Journal of Liability and Scientific Enquiry 2009 - Vol. 2, No.1 pp. 53 – 68.

Kouns, J. 2010, Ministry of Defence reports more than 1, 500 data loss incidents in the last five years, 15 Apr 2010, Seclist.org, http://seclists.org/dataloss/2010/q2/35

Kouns, J., 2010, ABC foul-up sees users' data exposed, 7 Oct 2010, Seclist.org, http://seclists.org/dataloss/2010/q4/2

Ponemon, (2009), 2009 Annual Study: French Cost of a Data Breach, Ponemon Institute, http://www.encryptionreports.com/

Price Waterhouse Cooper (2006), DTI Information security breaches survey 2006, http://webarchive.nationalarchives.gov.uk/tna/+/http://www.dti.gov.uk/files/file28343.pdf (Accessed 07 Oct 2010)

Price Waterhouse Cooper (2008), 2008 Information Security Breaches Survey, http://www.bis.gov.uk/files/file45713.pdf (Accessed 07 Oct 2010)

Singel, R., Probe Targets Archives‟ Handling of Data on 70 Million Vets, 1 Oct 2009, Wired.com http://www.wired.com/threatlevel/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/, (Accessed 07 Oct 2010)

Techweb, (2005), Seven-In-Ten Second-hand Hard Drives Still Have Data, Bank Systems and Technology, 01 Jul 2005, http://www.banktech.com/risk-management/showArticle.jhtml?articleID=165600008. (Accessed 07 Mar 2009)

Valli, C. (2004), Throwing out the Enterprise with the Hard Disk, In 2nd Australian Computer, Information and Network Forensics Conference, We-BCentre.COM, Fremantle Western Australia.

Verizon Business Risk Team, (2008), Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/databreachreport.pdf , (Accessed 07 Oct 2010).

Verizon Business Risk Team, (2009), 2009 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, (Accessed 21 Oct 2010)

Verizon Business Risk Team, (2010), 2010 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (Accessed 21 Oct 2010)

Von Bergen, (2010), Health insurers say data on 280,000 Pennsylvania clients may be compromised, The Philadelphia Inquirer, 20 Oct 2010. http://www.philly.com/inquirer/business/20101020_Health_insurers_say_data_on_280_000_Pennsylvania_clients_may_be_compromised.html#ixzz13LZbXlpk

Westervelt, R., (2009), Health Net healthcare data breach affects1.5 million, 19 Nov 2009, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1374839,00.html, (Accessed 07 Oct 2010)